Massive NSA operation exposed as Congress prepares vote on domestic spying bill

Bill Van Auken
11 March 2008

As the Democratic-led House of Representatives prepares to vote on legislation that essentially strips the American people of the constitutional protection from warrantless spying, the *Wall Street Journal* published an article Monday detailing the massive scale and intrusive character of the government's illegal surveillance operations.

The Senate has already passed—with substantial bipartisan support—domestic spying legislation that rubberstamps the Bush administration's demand for virtually unfettered wiretapping within the US. At the same time, the Senate bill provides retroactive immunity for telecommunications companies that violated their customers' privacy rights by collaborating in the government's illegal surveillance.

The House leadership is reportedly preparing to split these two aspects of the Senate legislation, in a cynical move designed to allow Democrats to approve the domestic spying powers, while most would cast a protest vote against immunity for the telecoms. Enough Democrats in the House have already indicated their support for immunity for this provision to clear the chamber as well.

The focus of the current congressional debate on immunity for telecommunications companies has served to obscure the police-state character of the domestic spying operation that this immunity is meant to protect.

Aborting the existing lawsuits—about 40 of which are currently before a San Francisco court—is intended to suppress the only legal means still available of uncovering information on the government's illegal spying. The Bush administration has fended off lawsuits against the government itself on the grounds that they would compromise "national security." The White House fears that civil suits against the companies would lead to disclosures that could form the basis for the criminal prosecution of the highest ranking members of the administration.

The *Wall Street Journal* article provides a revealing glimpse of what the administration is trying to hide.

The National Security Agency (NSA), without seeking any warrant or judicial supervision, is today monitoring "huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records," the *Journal* reports. "The NSA receives this so-called 'transactional' data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns."

The data defined as "transactional," and therefore supposedly not covered under constitutional protections against undue searches include e-mail records, including recipient and sender addresses, subjects and times sent; records of Internet sites visited and online searches made; numbers called on cell phones, both incoming and outgoing, the location of the phones and length of calls; numbers of incoming and outgoing calls on landline phones; individual financial data including on bank transactions and credit-card purchases and information on airline passengers.

Under the mantle of the NSA, the largest and most secretive of US intelligence agencies, the administration has maintained and expanded a vast data-mining operation that had previously been developed by the Pentagon—whose budget also covers the NSA. That program, known as "Total Information Awareness," was nominally disbanded after its existence was leaked to the press, triggering a political uproar and leading to a funding cutoff by Congress.

Any examination of the details of the revamped version of this program being carried out covertly by the NSA makes a complete mockery of the incessant claims by Bush and other administration officials that the domestic spying operation is directed solely at suspected Al Qaeda terrorists and those in communication with them.

On the contrary, it is a program that is sifting through and accumulating massive amounts of personal information on hundreds of millions of Americans.

According to the *Journal*, on the basis of analyzing this data, the NSA ferrets out "leads" to be pursued by various counterterrorism programs, including the NSA's own "Terrorist Surveillance Program," which is then empowered to wiretap phones and intercept e-mails between the US and overseas without court approval.

Even if it were true, as the NSA claims, that wiretaps are reserved only for such "leads," the collection of the "transactional" data represents a sweeping assault on the right to privacy and the Fourth Amendment of the US Constitution. By co-relating all of this various data, the government is able to assemble a revealing database containing confidential information on the private lives and activities of a huge segment of the American people, determining with whom and with what organizations they are in contact, what they buy, where they go and what their interests are.

Moreover, given the lack of judicial oversight, there is no reason to trust the NSA's account that such wiretapping is introduced only after a pattern determines grounds for suspicion of terrorist ties. Eavesdropping on phone calls and interception of e-mail is almost certainly directed at far wider sections of the population.

The *Journal* article provided a sense of the all-encompassing character of this data collection program carried out in the name of a universal "war on terrorism."

The paper reports: "Two former officials familiar with the data-sifting efforts said they work by starting with some sort of lead, like a phone number or Internet address. In partnership with the FBI, the

systems then can track all domestic and foreign transactions of people associated with that item—and then the people who associated with them, and so on, casting a gradually wider net. An intelligence official described more of a rapid-response effect: If a person suspected of terrorist connections is believed to be in a US city—for instance, Detroit, a community with a high concentration of Muslim Americans—the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city.

"The haul can include records of phone calls, email headers and destinations, data on financial transactions and records of Internet browsing. The system also would collect information about other people, including those in the US, who communicated with people in Detroit."

So much for the claims by Bush that his administration's massive surveillance program is directed only at "terrorists overseas." On the contrary, according to this account, the suspicion that a single terrorist might be in the city of Detroit would lead to a wholesale electronic dragnet being imposed over the entire metropolitan area, surveying not only the communications of the millions of people who live there, but also those of millions of others who call or e-mail them from other areas.

If this account is true, it directly contradicts previous claims by the Bush administration, including statements by the current director of the CIA, and former head of the NSA, Michael Hayden. Speaking on the NSA program in January 2006, Hayden insisted that it "is not a drift net over Dearborn or Lackawanna or Freemont grabbing conversations that we then sort out.... This is targeted, this is focused. This is about al Qaeda."

The *Journal* article further reveals that the source of concern on the part of both the administration and the telecoms that lawsuits over the data-mining operation be suppressed stems from the fact that companies "are giving the government unlimited access to a copy of the flow of communications, through a network of switches at US telecommunications hubs that duplicate all the data running through it." The paper adds, "It isn't clear whether the government or telecom companies control the switches, but companies process some of the data for the NSA, the current and former officials say."

Last week, three subcommittee chairmen of the House Energy and Commerce Committee issued a statement urging the House to put off any action on legislation granting blanket retroactive immunity to the telecoms. They cited the testimony of another whistleblower, Babak Pasdar, a security consultant to a major wireless carrier, who reportedly discovered a secret "Quantico Circuit" apparently providing the government with unrestricted access to all of their customers' voice communications and electronic data. Quantico, Virginia, is the site of major US Marine, FBI and Drug Enforcement Agency installations.

The revelation was similar to one from former AT&T technician Mark Klein, who revealed the existence of a "secret room" at AT&T's San Francisco hub containing a powerful data-mining device capable of monitoring not only AT&T's customers but the entire Internet.

A former technology advisor to the Federal Communications Commission has also charged in a sworn document submitted on behalf of one of the lawsuits filed against the telecoms that between 15 and 20 such devices have been set up at major hubs around the country.

"When you put Mr. Pasdar's information together with that of AT&T whistleblower Mark Klein, there is troubling evidence of telecom misconduct in massive domestic surveillance of ordinary Americans," said Cindy Cohn, Legal Director of the Electronic Frontier Foundation (EFF), one of the main groups suing AT&T for violating its customers' rights by colluding in the illegal activates of the NSA. "Congress needs to have hearings and get some answers about whether American telecommunications companies are helping the government to illegally spy on millions of us. Retroactive immunity for telecom companies now ought to be off the table in the ongoing FISA debate."

The Democratic Party leadership, however, has no interest in a political confrontation with the Bush administration on this issue. Their party is now in the midst of a bitter contest for the presidential nomination in which both candidates are vying to prove themselves qualified as "commander-in-chief." The Clinton camp, in particular, has begun employing the same kind of fear-mongering rhetoric that has been used by the Bush administration to promote and defend the domestic surveillance operation. Indeed, much of this spying began years before the September 11, 2001, attacks and was initiated under the Clinton administration.

Since taking control of both houses of Congress more than a year ago, the Democrats have held no hearings on domestic spying or sought in any way to expose the NSA program. There can be no doubt that leading Democrats are well aware that the Bush administration is lying through its teeth on the extent of its spying operations. The public finds out about these programs, however, only through occasional revelations in the newspapers—revelations that are quickly dropped by the media.

Like the Republicans, the Democratic leadership fully accepts the legitimacy of the overall framework of "national security" and the "global war on terrorism" used to justify the illegal spying carried out against the American people.

Whatever concerns they have expressed about this program, none of the leading Democrats have pointed to the obvious danger—that the massive intelligence being collected by the administration will be used to prepare wholesale repression under conditions in which social polarization, economic crisis and mass opposition to war will create political upheavals.